Data Communication & Client Server Architecture

Network: Connectivity of two or more nodes with the help of wired or wireless media for transmission of data is known as Network.

Networking: It is a process by which a network can be established or maintained.

Internetworking: It is a process by which two or more different network that are based on different subnet of IP address and these networks have been established at same physical location or remote physical location are connected to each other. These locations are known as sites.

Intranet : It is a combination of different networks related to same organization. Ex. – Railway, Defence, Banks, etc.

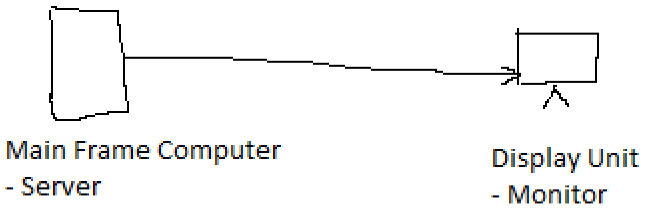
Internet : It is a combination of different networks related to different organization.

Connection Type of nodes :

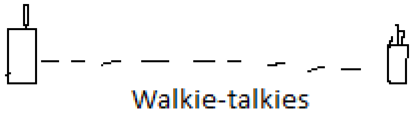
1. **Point-to-point** - Two nodes are connected to a specific link. The whole bandwidth of this link is use by connected two nodes only. Ex. Connection between two laptops, computer connected to a switch, etc.
2. **Point-to-multipoint** – One node is connected to multiple nodes by sharing / dividing the bandwidth of the link. Ex-Connection of multiple branches of a bank to zonal office.

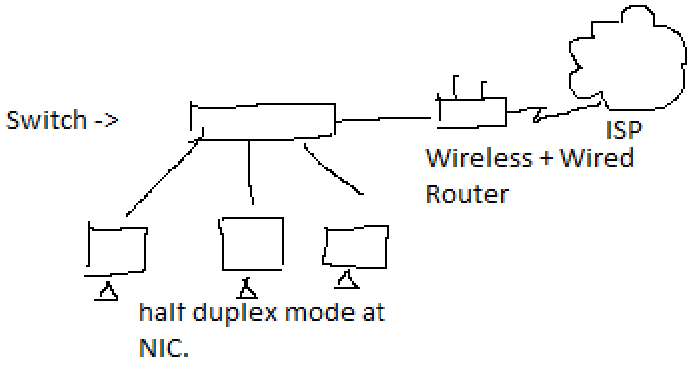
Data Flow :

1. **Simplex** - In this transmission sender node always sends data and receiver node only receives data. Ex – Television, Mainframe computer to monitor

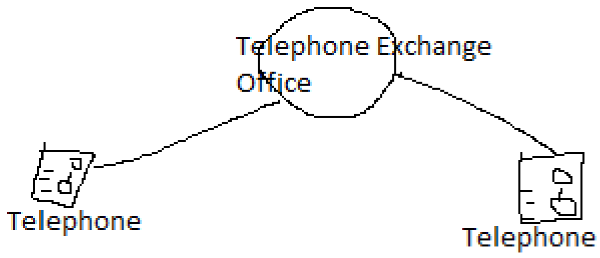


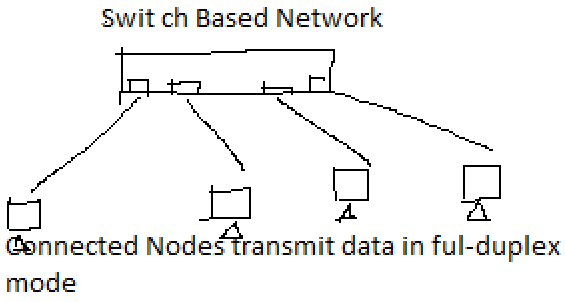
2. **Half Duplex** – In this transmission sender and receiver both can send and receive data but only one task can be done one time. Ex – Walkie-Talkies , Hub





3. **Full Duplex** – In this transmission both sender and receiver can send and receive data at the same time. This is based on channel of transmission medium. Ex- Telephone, Computer, Switch





Topology : A network represents connectivity of nodes that is based on physical and logical structure. This structure is known as topology.

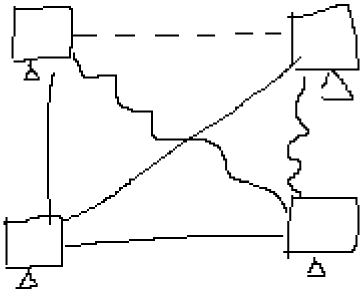
Basic Types of topology :

1. **Logical Topology** : It represents the configuration of nodes for different services. Like – OS installation, Services configuration, Logical Addressing (IP address), etc.
2. **Physical Topology** : It represents the arrangement of nodes connected to wired or wireless medium.
   Types of Physical Topology :
   1. **Mesh Topology**
      Important Points :
      a. Each Device is connected to all another device through a dedicated link – point to point connection
      b. Less data traffic load
      c. Failure of one link does not affect another device

d. It difficult to establish and manage because it requires many links and input / output network ports.

e. Link Calculation – No. Of nodes (n) = 4
No. of link to each node = n-1 = 4-1 = 3
No. Of total link = n(n-1) / 2 = 4(4-1) / 2 = 6

f. Ex – Telecommunication



Mesh Topology

2. **Bus Topology**

Important Points :

a. All nodes are connected to a single wire (known as back bone cable).

b. Coaxial Cable is used as a back bone cable.

c. BNC connector is used to at nodes to back bone cable.

d. With the help of BNC , a drop line is created and nodes are connected.

e. At the end of cable Terminator is to used to stop lose of signal.

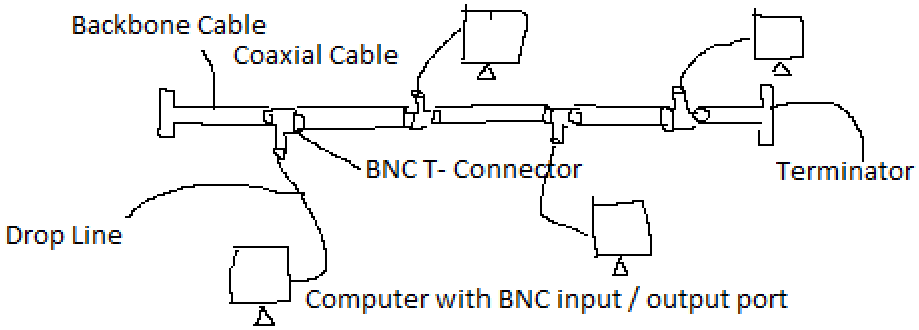
f. It is easy to establish because it requires less cable and input / output ports.

g. Damage into backbone cable causes failure of connectivity of nodes because break part of cable generates noise for all nodes.

h. Difficult to add a new node.

i. Collision of data is very high.

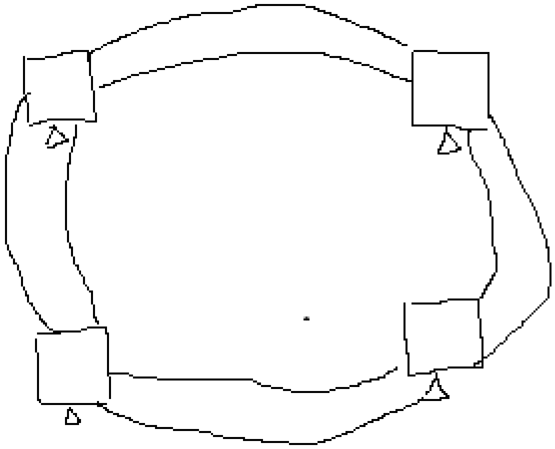
j. It works on CSMA / CD technique.
k. Ex – Cable TV
l. Each node has information about next node. So, It is known as partial ring topology.
m. It is also known as partial ring topology because each node keeps information about next node.



3. Ring Topology

Important Points :

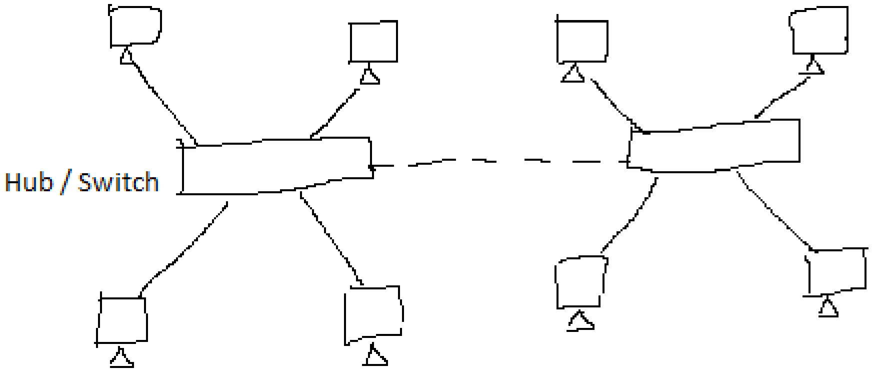
a. Each node is connected to neighbour nodes that forms a ring based structure.
b. Connection can be based on single ring and dual ring.
c. It works on Token Ring Passing technique in which a logical token is transferred from one node to another node. Token is grabbed by the sender node. Sender node add source and destination address with token and released. All data packets are attached behind token. Destination Node accepts this token and extract all attached data packets.
d. It reduces data confliction.
e. Max. Two links are used.
f. It is very slow.



4. **Star Topology**

   Important Points :

   a. In this topology each node to connected to a central device that is known as MAU (Multiple Access Unit). MAU can be Hub or Switch.
   b. Each node is connected to MAU with separate link.
   c. Performance of this topology depends upon MAU and link quality.
   d. If problem occur with any node, it does not affect another nodes means reliability is very high.
   e. It is most commonly used topology in LAN.



Star Topology

5. Wireless Topology

Important Points :

a. In this topology, unguided media is used.
b. It works on frequency. Commonly in LAN – 2.4 GHz or 5 GHz
c. All nodes are connected to a central device that is known as AP (Access Point)
d. AP name is known as SSID (Security Set Identifier)
e. This topology can be extended easily.
f. Wireless Security Protocols :

Wired Equivalent Privacy (WEP)
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Access 2 (WPA 2)
Wi-Fi Protected Access 3 (WPA 3)

WEP (Wired Equivalent Privacy) – It was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure. Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

WPA (Wi-Fi Protected Access)- For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP (/tiːˈkɪp/) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion. The attacks that posed the most threat to the protocol were however not the direct ones, but those that were made on Wi-Fi Protected Setup (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

WPA2 (WPA version 2)

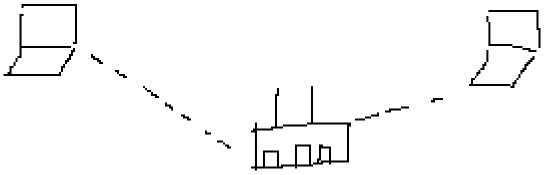
The 802.11i wireless security standard based protocol was introduced in 2004. The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES). AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.

ADVANCED ENCRYPTION STANDARD IS APPROVED BY THE U.S.

GOVERNMENT

At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured WiFi network and can gain access to certain keys to perform an attack on other devices on the network. This being said, the security suggestions for the known WPA2 vulnerabilities are mostly significant to the networks of enterprise levels, and not really relevant for small home networks.

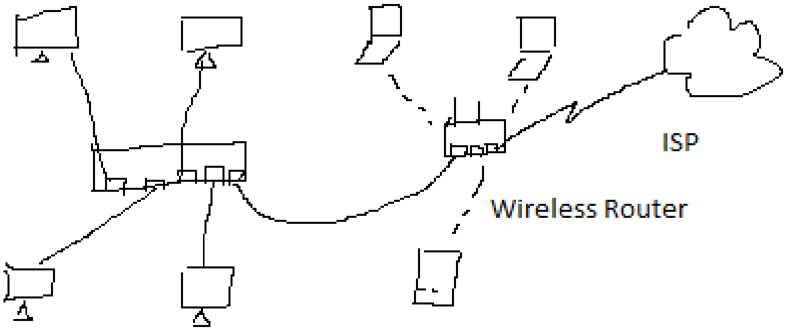
Unfortunately, the possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too. And even though breaking into a WPA/WPA2 secured network through this hole will take anywhere around 2 to 14 hours it is still a real security issue and WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector.



Wireless Router

6. Hybrid Topology

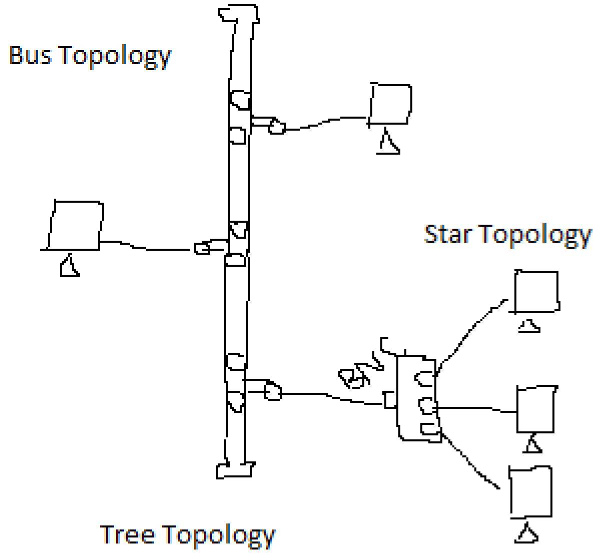
It is just the combination of two or more topologies.



Hybrid Topology

7. Tree Topology

It is combination of Bus and Star topology.



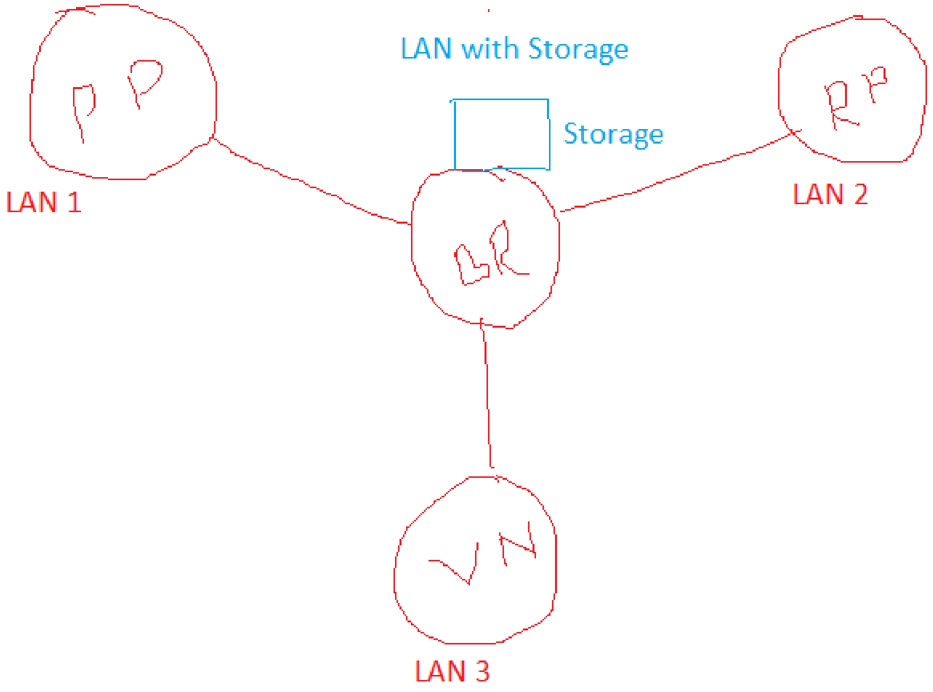
Categories of Network :

1. **LAN**
   A network that has been established in a small area like small office, corporate office, building or campus is known as LAN (Local Area Network). It is mostly based on twisted pair cable or wireless.

2. **MAN**
   A network that has been established in a large city (Metropolitan City) like Internet connection, government project etc. Is known as MAN (Metropolitan Area Network). It can be based on Optical Fiber Cable or Frequency.

3. **WAN**
   A network that has been established in very large area like country or world. It is mostly combination of multiple organizations network. Ex. – Internet
4. **SAN (Storage Area Network)**

A network that is used to store huge amount of data is known as SAN.



5. CAN (Campus Area Network)
6. PAN (Personal Area Network)

Basic Concept of Devices :

The above transmission of data, topology and network models are developed with the help of few devices :

1. **NIC (Network Interface Card) / LAN Card / Network Card /Ethernet Card**

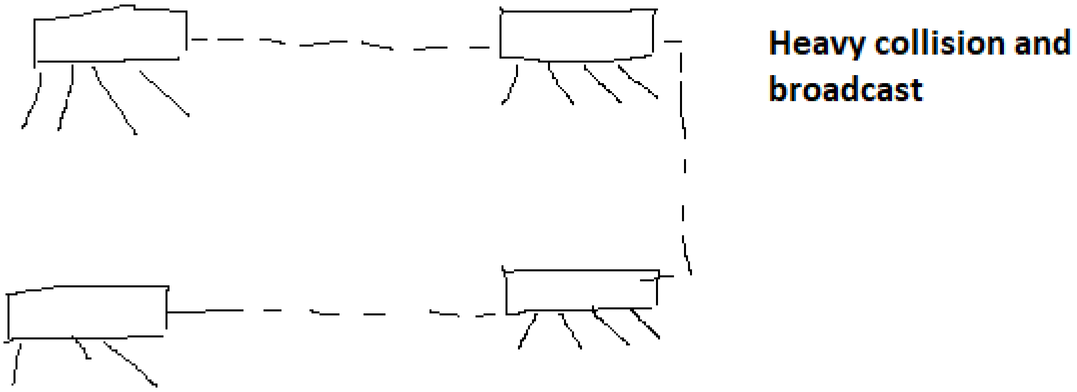
a. Works at layer 2 – Data Link layer
b. Used to connect a node with another node or network
c. Types – wired , wireless
d. At wired NIC RJ-45 port is available with 8 pins
e. Wireless NIC works at frequency (Radio Frequency)
f. NIC has a ROM in which MAC address is present. So, MAC address is known as Physical Address.
g. By default NIC works in auto mode while it can be set for Half Duplex or Full Duplex mode.
h. Mostly NIC is with fixed with mother board. In case of extra NIC, it is attached with PCI slots.

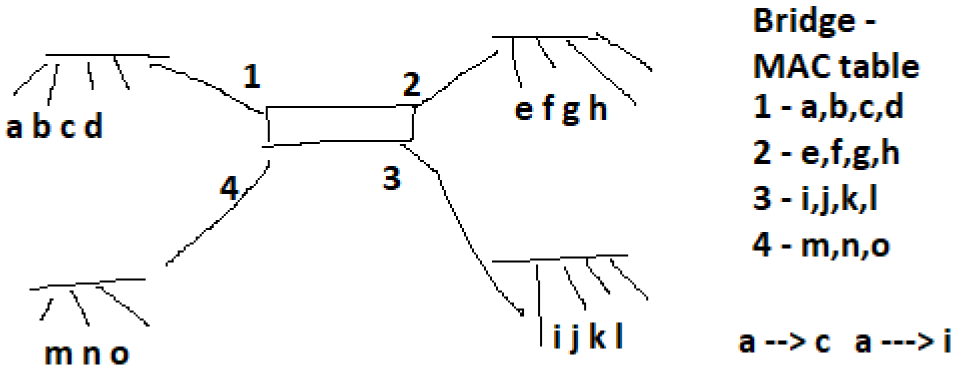
2. Hub

a. Hub is used in star topology
b. It just connect multiple nodes as a connector
c. Works at physical layer
d. RJ – 45 ports - 4, 8,16,24
e. Heavy collision and broadcasting
f. It works in half duplex mode
g. Maximum speed – 10 Mbps
h. Types of HUB – Active , Passive
Passive – Data signal is weak
Active – Works as multiport repeater. Signal is regenerated at every port.

3. Bridge

a. Used in star topology based network.
b. OS based device
c. Creates MAC address table
d. It works at data link layer
e. Available with 2 or 4 RJ-45 ports
f. Reduces collision and broadcast
g. It is used to break a network into segments or to join multiple segments of network.





4. **Switch**
   a. This device is used in star topology based network.
   b. It is almost similar to Hub in structure.
   c. It has RJ-45 ports.
   d. It is available with 4, 8, 16, 24, 48, 96, 128 ports.
   e. Switches are available with 100Mbps, 1000Mbps or 10Gbps speed
   f. It works in full duplex mode
   g. Switch works at layer 2 and layer 3 both. So, Switches are also known as Layer 2 or 3 switch.
   h. It has multiple broadcast domain and collision domain. But switch initially works in single broadcast domain till the learning of MAC address.

i. It creates MAC Table / CAM table /Filter Table

Types of Switch :

1. **Unmanageable Switch –** It is just plug and play device. It cannot be configured.
2. **Manageable Switch –** It can be configured for port management, IP address configuration , security, etc.

5. **Router**
   a. Router is used for communication between two or more different network that are based on different subnet of IP address.
   b. It is a Layer 3 device.
   c. It is an OS based device.
   d. It creates routing table in which it keeps best route information for different destination network.
   e. It can filter data packets.
   f. It has different types of ports like Fast Ethernet, Gigabyte Ethernet, serial port, ISDN port, Console port, etc.

Types of Router :

1. **De-modular Router –** Its all ports are fixed with router. Ex. – Model 2520
2. **Modular Router –** Its few ports are fixed with router and some free slots are available to attach different types of cards. Ex. – Model 1841, 1941, 7200, 900, 901

6. **Firewall**
   a. This device is used for security in the network.
   b. It can filter data packets.
   c. It allows or restricts different sites.
   d. It can also route data packets.
   e. It is an OS based device.

f. It can be implemented at the boundary of network or in the middle of network.
g. It has different types of ports like router.
h. Ex – ASA 5500

7. **Access Point**
   a. This device is used to create a wireless network.
   b. It generates signal through which wireless devices are connected to it.
   c. It has internet port, fast Ethernet or Giga Byte Ethernet ports.
   d. It supports MAC filtering, Port forwarding, speed control, data use limitation, etc.

Media

A path through which data can be transmitted.

Types – Guided Media – Wired Communication

Unguided Media – Wireless Communication

Frequency based data transmission.

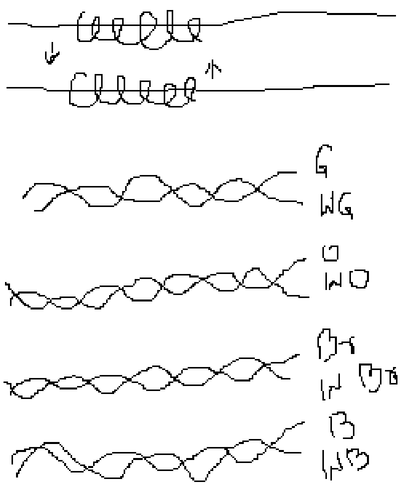
Network Cables

1. Twisted Pair Cable (TPC)
   a. 4 pair Cable – 8 cables
   b. Based on Ethernet Technique (IEEE – 802.3)
   c. Uses – Computer Network, CCTV, Telephone, Wi-Fi devices, V-SAT
   d. Speed – up to 1 Gbps
   e. Distance Coverage – up to 100m
   f. Connector – RJ-45 (RJ- Registered Jack) – 8 pins
      RJ-11 - 4 pins (Modem, Tel. Set)
   g. Categories – cat1,2,3,4,5,5e,6,6a,7
   h. Types –
      1. STP – Very less effect of EMI
      2. UTP - High effect of EMI

i. Cable Color code given by TIA/EIA
   a. Pair 1 – Orange, White Orange
   b. Pair 2 – Blue, White Blue
   c. Pair 3 – Green, White Green
   d. Pair 4 – Brown, White Brown
   Total pairs 4 = 8 wires

j. Twisted Pair Cable pairs are managed to create different cable as per used by arranging is cable color –
   1. Straight Over Cable – Used to connect dissimilar devices like – Computer to hub or switch, Router to switch, firewall to switch/router
   2. Cross Over Cable – Used to connect similar devices like – Router to Router, Hub to Hub, Switch to Switch, PC to PC
   3. Roll Over Cable – Used to connect Router, Firewall or Switch with PC for configuration
      Now, the above cables are based on sequence of color of cable in the connector.

Why twisting is done with TPC?

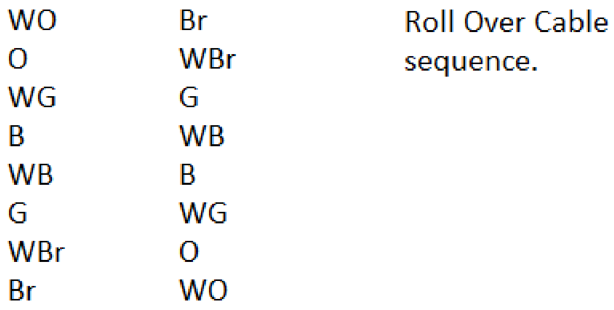


TIA/EIA has given few standard for sequencing of cable –

TIA/EIA-T568A			TIA/EIA-T568B	
1	WG		1	WO

2	G		2	O
3	WO		3	WG
4	B		4	B
5	WB		5	WB
6	O		6	G
7	Br		7	Br
8	WBr		8	WBr

1. Straight Over Cable –
   Use 568A or 568B rule at both end of cable.
2. Cross Over Cable –
   Use 568A rule at one end and 568B rule at another end.
   OR,
   Use 568B rule at one end and 568A rule at another end.
3. Roll Over Cable –
   We can use 568A or 568B rule at one end but at another end just opposite the position of cable.



WO	Br	Roll Over Cable sequence.
O	WBr	
WG	G	
B	WB	
WB	B	
G	WG	
WBr	O	
Br	WO	

Patch Code – Industry manufactured TPC with connector.
Practical - RJ45 plug on UTP cable - Installing - YouTube

Coaxial Cable:-

1. Single copper wire.
2. Proper shielded
3. Connector – BNC
4. Distance Coverage – up to 500m
5. Speed – 10Mbps
6. Uses – Cable TV, Bus Topology based network, CCTV

7. Types:
    a. RG-58 / Thick Coaxial Cable / 10Base5
    b. RG-59 / Thin Coaxial Cable / 10Base2
8. To connect PC with coaxial cable, PC must have BNC port.

Optical Fiber Cable / Fiber Optic Cable (OFC)/Fiber Cable

1. Light – Laser / LED
2. Small Diameter
3. Works on total internal reflection
4. Glass / Fiber
5. Long distance
6. Speed high
7. Flexible -
8. Bandwidth high
9. Costly
10. Light moves in straight line
11. Tough use
12. Very less effect of EMI
13. Patch Code

What is protocol?

It is a set of rules and instructions which is responsible to execute a specific process.

Initially protocols are platform dependent.

To make protocols platform independent, TCP/IP Model was developed by Department of Defense of America. So, It is also known as DOD model.

It has 4 / 5 layers :

4 Application – OSI Ref. Model –App, Pre, Session
Protocols – DNS, DHCP, HTTP, HTTPs, POP3, IMAP
3 Transport - Protocols –TCP, UDP

2 Internet - OSI Ref. Model – Network Layer

Protocols – IP, ICMP,

1 Network Interface – OSI Ref. Model – Data Link & Physical Layer

MPLS, Ethernet, Frame Relay, ATM,

OR,

5 Application

4 Session

3 Transport

2 Network

1 Physical

To explain TCP/IP model in more detail, OSI Model was developed.

So, it is also known as OSI Reference Model.

Protocols –

1. HTTPs (Hyper Text Transfer Protocol with SSL(Secure Socket Layer) - 443
   Used for web page accessing with security
2. HTTP (Hyper Text Transfer Protocol) - 80
   Used for web page accessing without security
3. FTP (File Transfer Protocol) – 20,21

4. DHCP (Dynamic Host Configuration Protocol) – 67,68
   Used to provide IP address automatically and dynamically to client machines as per configuration.
   Practical:
5. DNS (Domain Name Service / System) - 53
   Used to convert Domain name to IP address and vice versa
   Practical:
6. SMTP (Simple Mail Transfer Protocol) - 25
   Used for mail service. In mail service, it is used to transfer mail.

7. POP3 (Post Office Protocol version 3) - 110
   Used to receive mail. In case of Outlook, it cuts mail from mail server and download it on local machine.
8. IMAP4 (Internet Message Access Protocol) - 143
   Used to receive mail. In case of Outlook, it copies mail from mail server and download it on local machine.
9. Telnet (Tele Comminication) - 23
   It is used to access a machine remotely through command line.
   Practical:
10. RDP (Remote Desktop Protocol)
    It is used to access a machine remotely with GUI.
    Practical:
11. SSH (Secure Shell) -22
    It is used to access a machine remotely with command line. It provides high security with MD5 (Message Digest version 5) encryption.
12. TCP (Transmission Control Protocol)
    Used for reliable data transmission with acknowledgement.
13. UDP (User Datagram Protocol)
    Used for unreliable data transmission without acknowledgement.
14. IP (Internet Protocol)
    It is used to provide unique identity to network nodes. With this identity, two or more nodes of a network or different network can communicated to each other.
    Version – IPv4, IPv6
15. ICMP (Internet Control Message Protocol) - 1
    It is used to send and receive data packetes to check connectivity with destination node.
    Practical:
16. ARP (Address Resolution Protocol)
    It resolves MAC address with IP address.
    Practical:

17. WAN Technics –Leased Line, ISDN
Frame Relay, ATM, MPLS, VoIP

Characteristics of OSI Model

Here are some important characteristics of the OSI model:

- A layer should only be created where the definite levels of abstraction are needed.
- The function of each layer should be selected as per the internationally standardized protocols.
- The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.
- In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer
- Changes made in one layer should not need changes in other lavers.

Why of OSI Model?

- Helps you to understand communication over a network
- Troubleshooting is easier by separating functions into different network layers.
- Helps you to understand new technologies as they are developed.
- Allows you to compare primary functional relationships on various network layers.

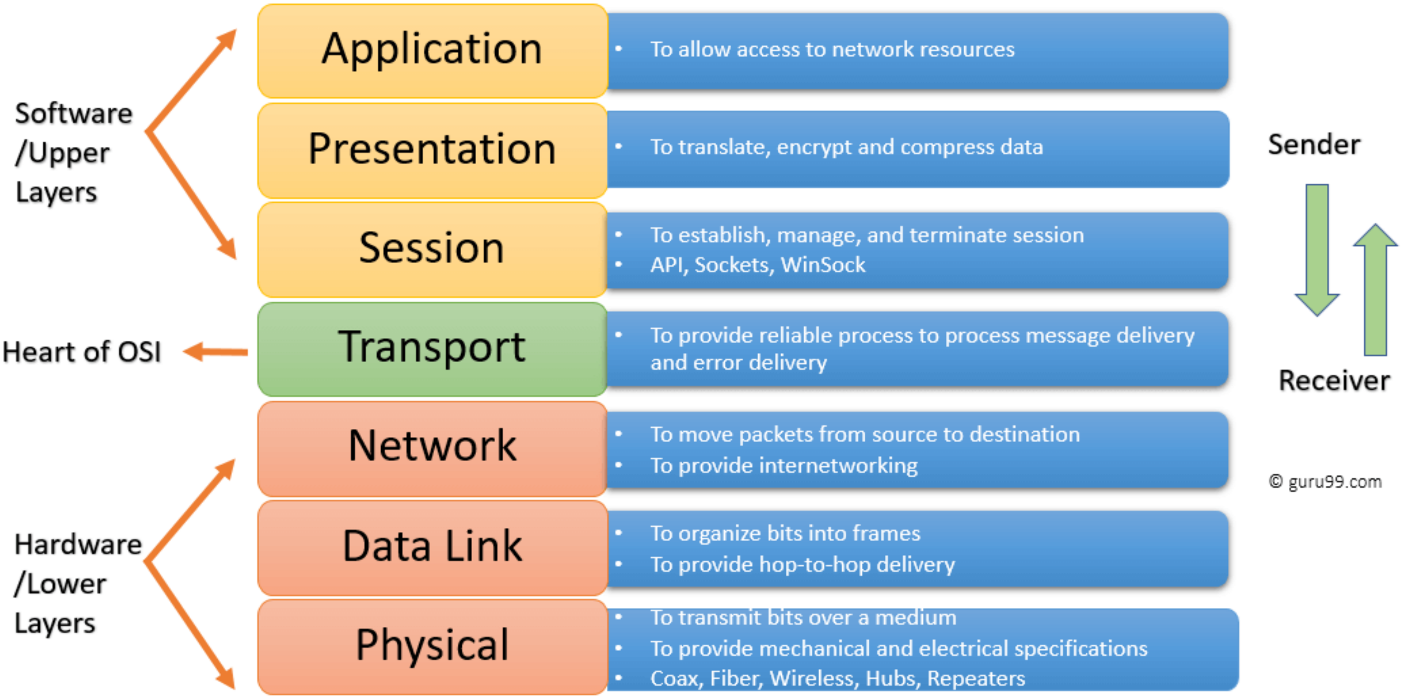
History of OSI Model

Here are essential landmarks from the history of OSI model:

- In the late 1970s, the ISO conducted a program to develop general standards and methods of networking.

- In 1973, an Experimental Packet Switched System in the UK identified the requirement for defining the higher-level protocols.
- In the year 1983, OSI model was initially intended to be a detailed specification of actual interfaces.
- In 1984, the OSI architecture was formally adopted by ISO as an international standard

7 Layers of the OSI Model


Software /Upper Layers
Heart of OSI
Hardware /Lower Layers
Application
To allow access to network resources
Presentation
To translate, encrypt and compress data
Session
To establish, manage, and terminate session
API, Sockets, WinSock
Transport
To provide reliable process to process message delivery and error delivery
Network
To move packets from source to destination
To provide internetworking
Data Link
To organize bits into frames
To provide hop-to-hop delivery
Physical
To transmit bits over a medium
To provide mechanical and electrical specifications
Coax, Fiber, Wireless, Hubs, Repeaters
Sender
Receiver
© guru99.com

Physical Layer

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

Few important Points:

a. Physical characteristics of interfaces and medium
b. Representation of bits
c. Data rate
d. Synchronization of bits
e. Line configuration
f. Physical topology
g. Transmission mode

Data & Signal

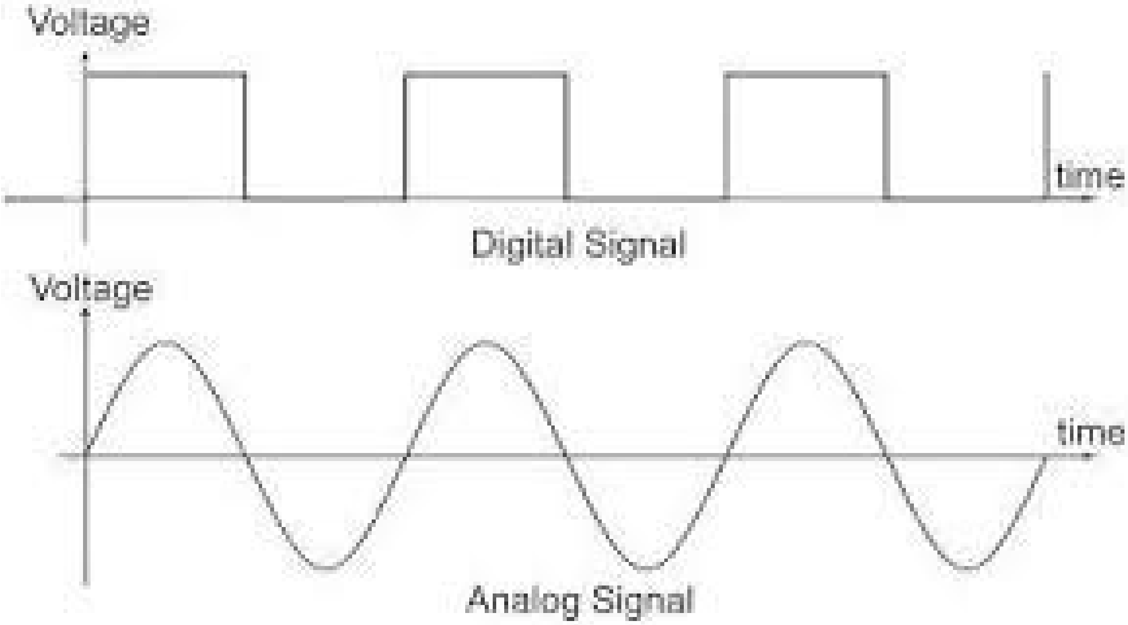
Data can be analog or digital that communicate at a medium or stored at a device.
Analog Data - Continuous flow of data like voice.
Digital Data - Break in the flow of data like data stored in the computer in the form of 0's and 1's.
Signal : It is carrier of data.

Analog Signal :

1. It has infinite number of values.
2. It has continuous flow of electrical signal.
3. It is represented into sine waves.

Digital Signal :

1. It has only 2 values that is 0's and 1's.
2. It has non-continuous electrical signal.
3. It is represented into square waves.



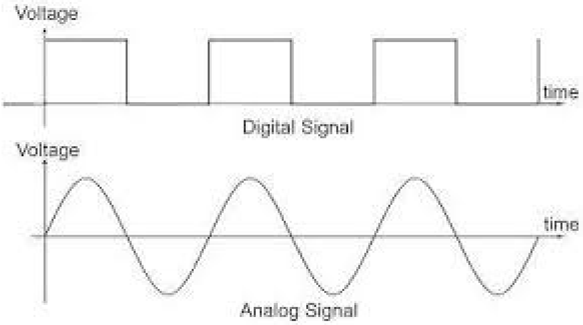
Periodic and non-periodic / Aperiodic Signal

Both analog and digital signal can be periodic and non-periodic signal.

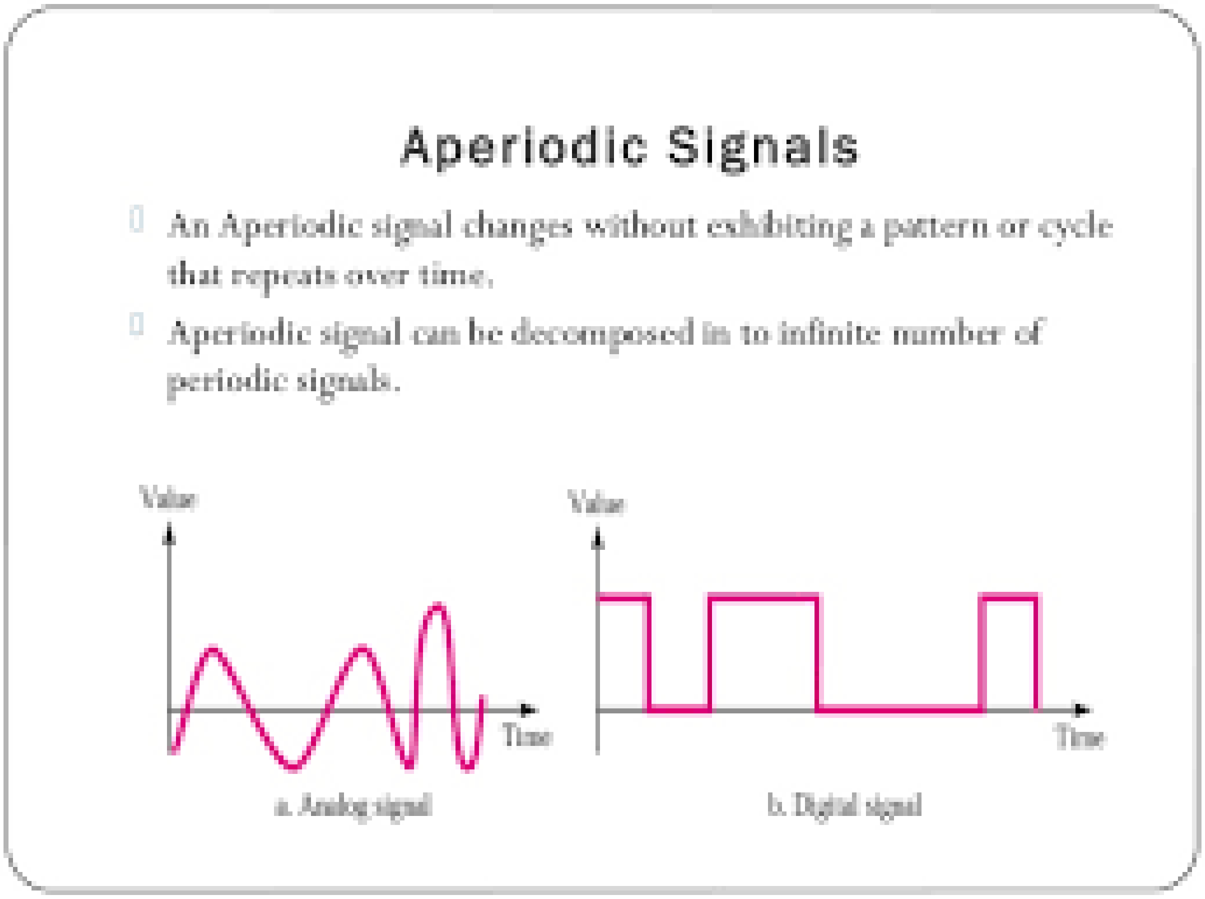
A periodic signal completes the same cycle at fixed interval of time.

A non-periodic signal does not complete its cycle at fixed interval of time.

Example of periodic signal :



Example of non-periodic signal :



Aperiodic Signals

- An Aperiodic signal changes without exhibiting a pattern or cycle that repeats over time.
- Aperiodic signal can be decomposed in to infinite number of periodic signals.

Few Properties of Sine Wave (Analog Signal):

1. Amplitude : The highest peak of signal is known as its amplitude. In case of electrical signal it is measured in Volt (V).
2. Period : One cycle of signal is known as 1 period. It is measured in Second.
3. Frequency : Number of period in 1 S. It is measured in Hertz (Hz).

Notes : Frequency and period are the inverse of each other.

f=1/t or t=1/f

Unit	Equivalent	Unit	Equivalent
Seconds(S)	1s	Hertz (Hz)	1Hz

Millisecnds(ms)	10-3s	Kilohertz(KHz)	10^3 Hz
Microseconds(ms)	10-6s	Megahertz(MHz)	10^6 Hz
Nanoseconds(ns)	10-9s	Gigahertz(GHz)	10^9 Hz
Picoseconds (ps)	10-12s	Terahertz(THz)	10^12 Hz

4. Wavelength : Distance between two crests or troughs is known as wavelength. It is measured in lamda.
5. Phase : Two or more waves with same frequency, amplitude and wavelength but its point of generation degree is different.
6. Single Sine Wave - It is a single signal means only one sine wave is generated from one device to another. It is used to carry electric supply, alarm etc.
7. Composite Signal - It is a combination of multiple sine waves. It type of signal is used to carry data.

Few properties of Digital Signal

1. Uses electric low and high voltage to represent data.
2. Data is represented in 0's and 1's.
3. Speed of digital signal is measured in bits per seconds that is known as bit rate.
4. Low Pass Channel - A channel that starts with 0.

Bandwidth :

The range of frequencies contained in a composite signal is its bandwidth.

The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000.

Throughput:-
The throughput is a measure of how fast we can actually send data through a network.
Although, at first glance, bandwidth in bits per second and throughput seem the same,
they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps
through this link with *T* always less than *B.* In other words, the bandwidth is a potential
measurement of a link; the throughput is an actual measurement of how fast we can
send data. For example, we may have a link with a bandwidth of 10 Mbps, but the
devices connected to the end of the link may handle only 5 Mbps. This means that we
cannot send more than 5 Mbps through this link.

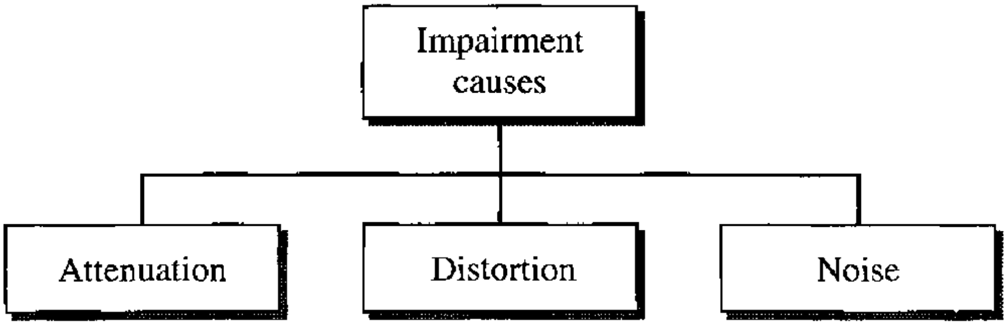
Baseband transmission –

1. Digital signaling.
2. Time division multiplexing is used
3. Baseband is bi-directional transmission by using TDM.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet – 10BaseT

Broadband transmission –

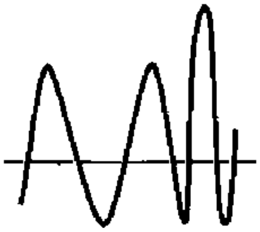
1. Analog signaling.
2. Frequency division multiplexing possible
3. Transmission of data is unidirectional by using FDM. FDM is used to create multiple channels.
4. Long distance signal travelling.
5. Bandwidth is divided into multiple channels.
6. Example : Used to transmit cable TV, Telephone, Radio Station, Fiber Optic Cable

Transmission Impairment : Simply we can say, it is disturbance with data signal during the transmission through medium. Due to impairment, data loss occurs.

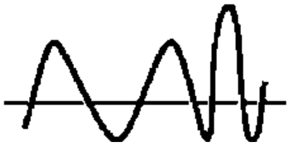


a. Attenuation -

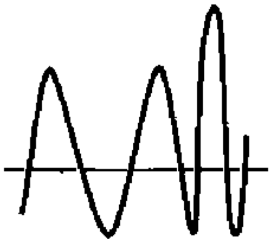
Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.



Original Signal



Attenuated Signal

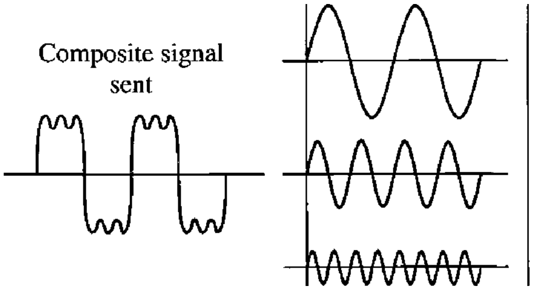


Amplified Signal

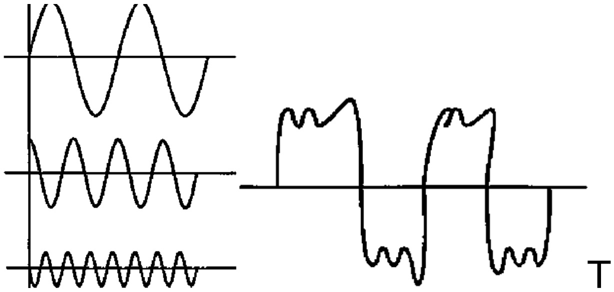
Note : Signal strength is measured in decibel (dB).

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies and phase. Each signal component has its own propagation speed through a medium. So, distortion may cause of delay in transmission and loss of data.



Three signals with different phases.

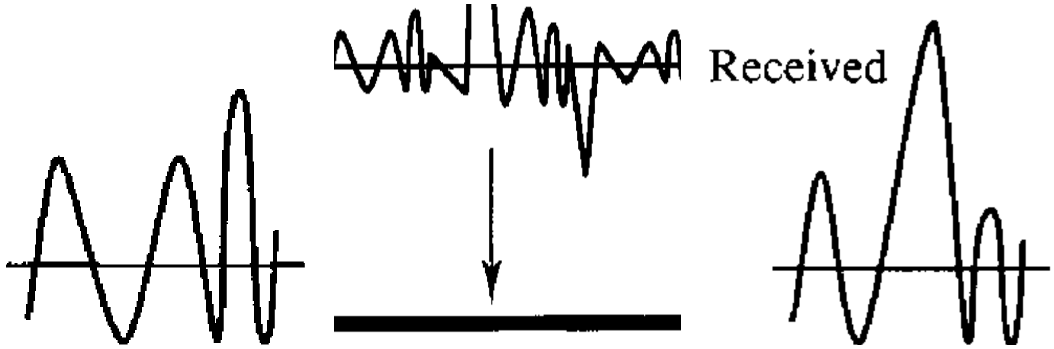


This is distorted received signal.

Composite Signal Received

Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.



Sent Signal Noise generated Distorted Signal

Digital Data over Digital SIgnal :

Line Coding :

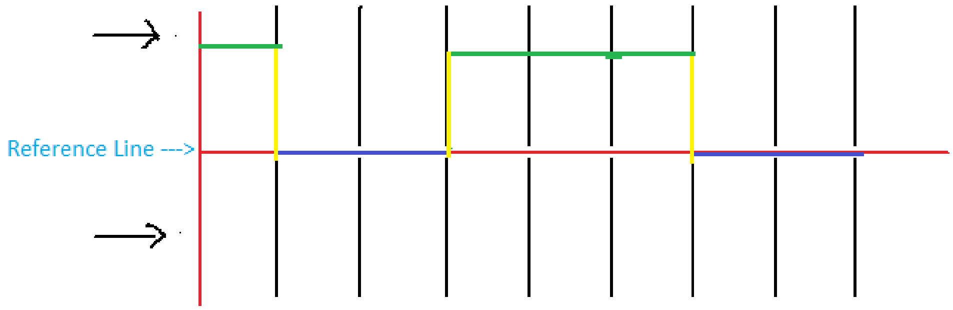
Putting digital data over digital signal is known as Line Coding.

There are 5 major categories of Line Coding :

1. Unipolar - NRZ
2. Polar - NRZ-L, NRZ-I, RZ, Manchester, Differential Manchester
3. Bipolar – RZ, AMI, pseudoternary
4. Multilevel - 2B/IQ
5. Multi transition - MLT-3

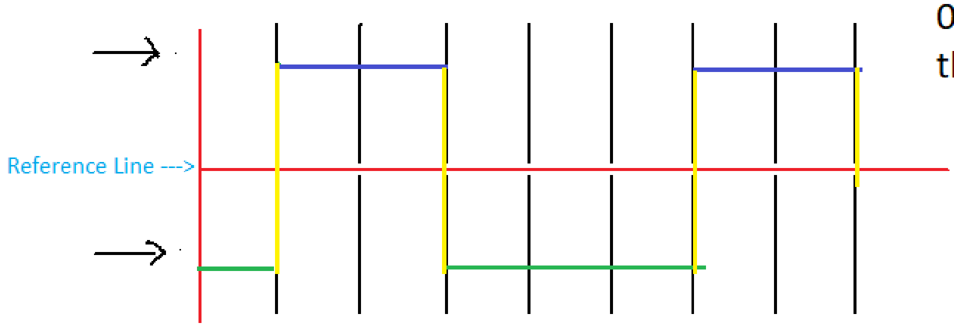
Example of few line coding:-

Digital Value - 10011100



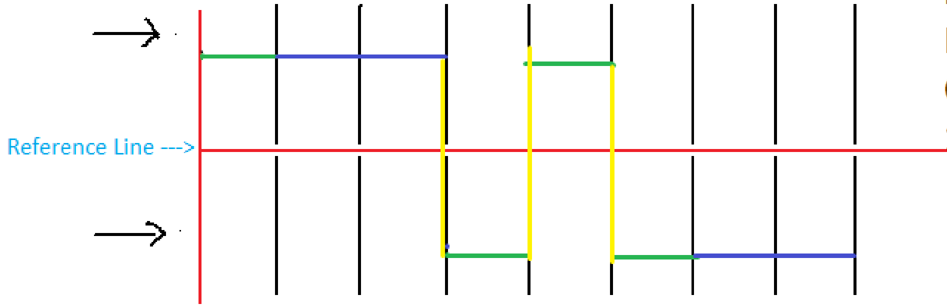
Unipolar - NRZ
(Non Return to Zero)
1 -> Above the Ref. line
0 -> On the Ref. line

Digital Value - 10011100



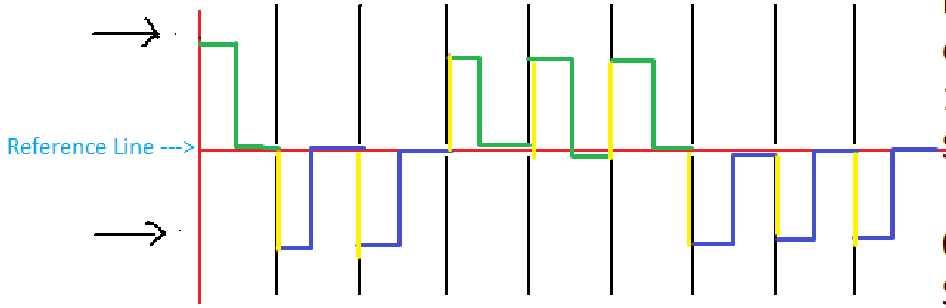
NRZ-L -> 1 is represented below the Ref. line.
0 is represented above the Ref. line.

Digital Value - 10011100

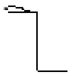


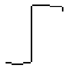
Polar - NRZ-I
O or 1 both can be represented above the Ref. line.
O - No Transition
1 - Transition

Digital Value - 10011100

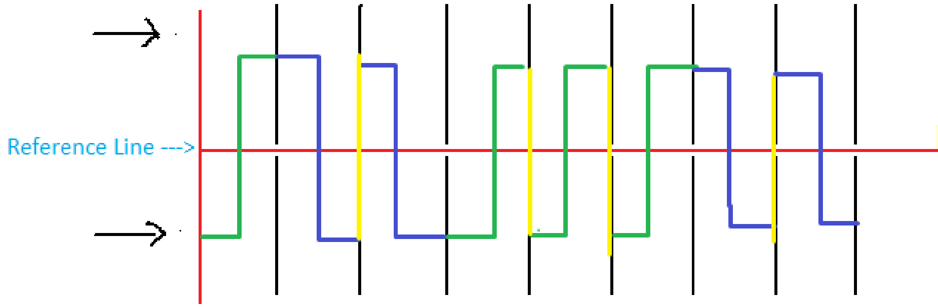


Polar - RZ(Return To Zero)
Transition will occour between the bit to represent every bits.

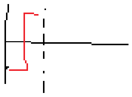
1 - Above the Ref. Line
Symbol - 

0 - Below the Ref. Line
Symbol - 

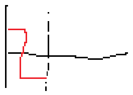
Digital Value - 10011100



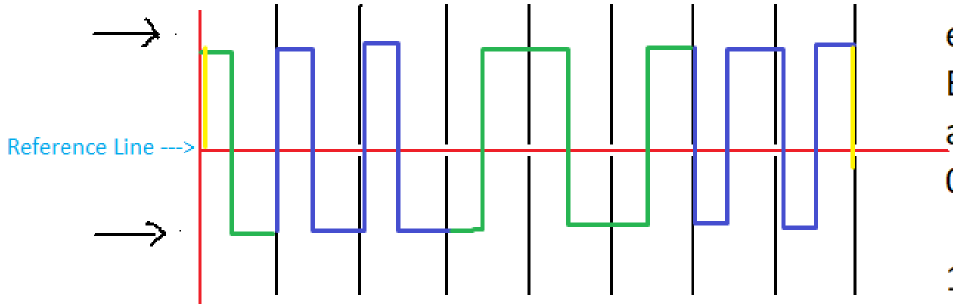
Polar-Manchester
(Based on IEEE-802.3)
Notes :- Above RL, +ve
Below RL , -ve
Every bit wil transite between bits.
Now,
1 - Transition -ve to +ve



0 - Transition +ve to -ve



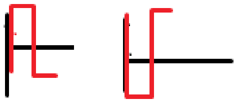
Digital Value - 10011100

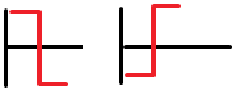


Polar - Differential
Manchester (D-Man)

Transition occour at every bit i.e. 0 ro 1

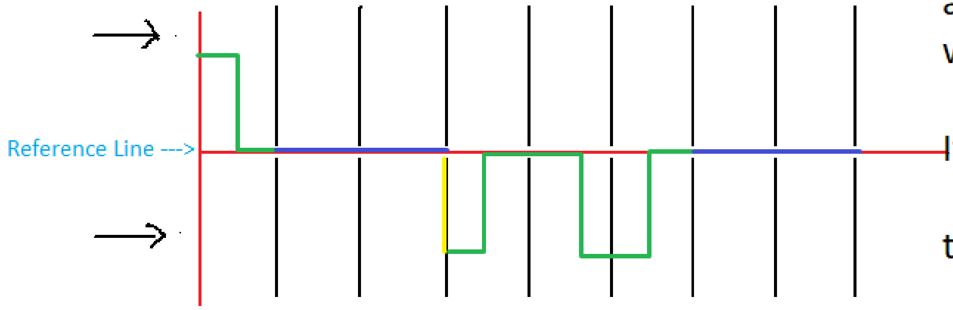
Both are represented above and below the RL.

0 - symbol 

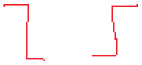
1 - Symbol 

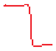
These symbols are used as per the situation.

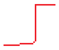
Digital Value - 10011100



Bipolar - RZ(Return To Zero)

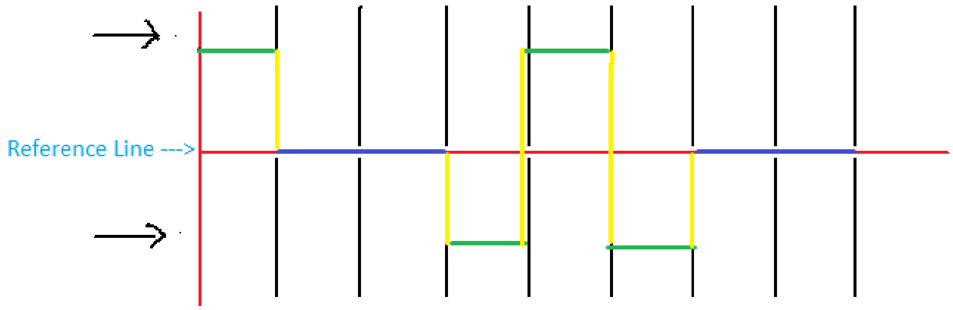
1 - It can be represented above or below the Ref. Line with symbol 

If first 1 is represented with 

then the next 1 is with 

0 - Always represented on the Ref. Line.

Digital Value - 10011100

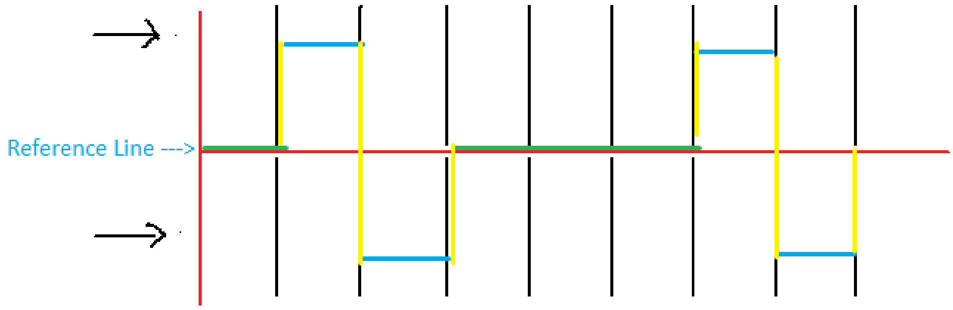


Bipolar- AMI or NRZ
AMI - Alternate Mark Inversion

0- Always represented at Ref. Line

1- represented above or below the RL. But it should be alternate means if first 1 is above the RL then second 1 will be below the RL then the next 1 will be above the RL and so on.

Digital Value - 10011100



Bipolar-Pseudoternary

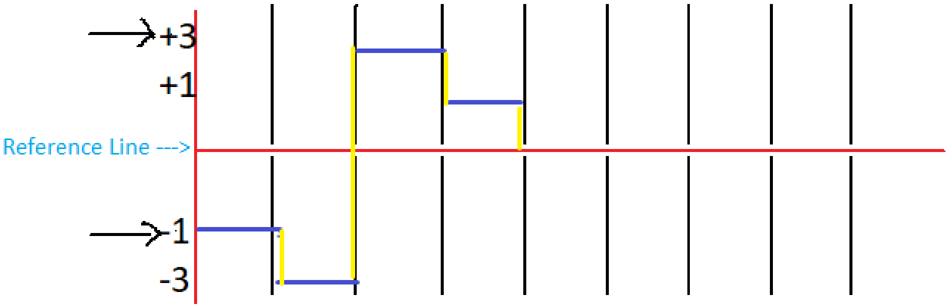
1 - It is always represented on the RL.

0 - It is represented above or below the RL but in alternate means if first 0 is above the RL then second 0 will be below the RL the next 0 will be above the RL and so on.

Note :- It is opposite of Bipolar-AMI

Digital Value - 10011100

Bits	Positive	Negative
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

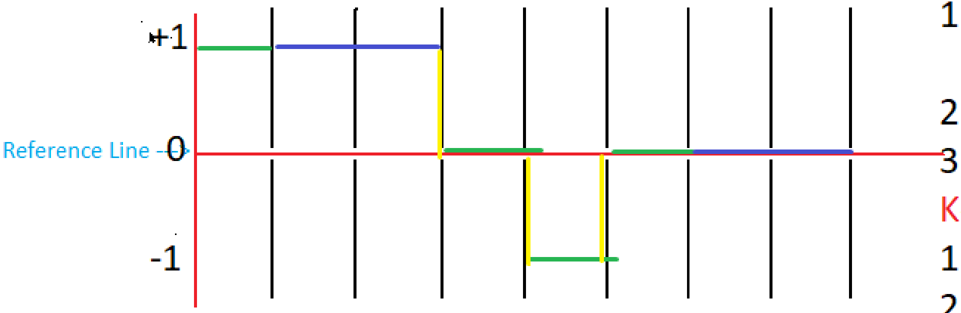


Multilevel - 2B1Q

Always start with positive then see the level of last taken value. As per the positive or negative level of last value take value from column.

Note:- Group data in two bits.

Digital Value - 10011100

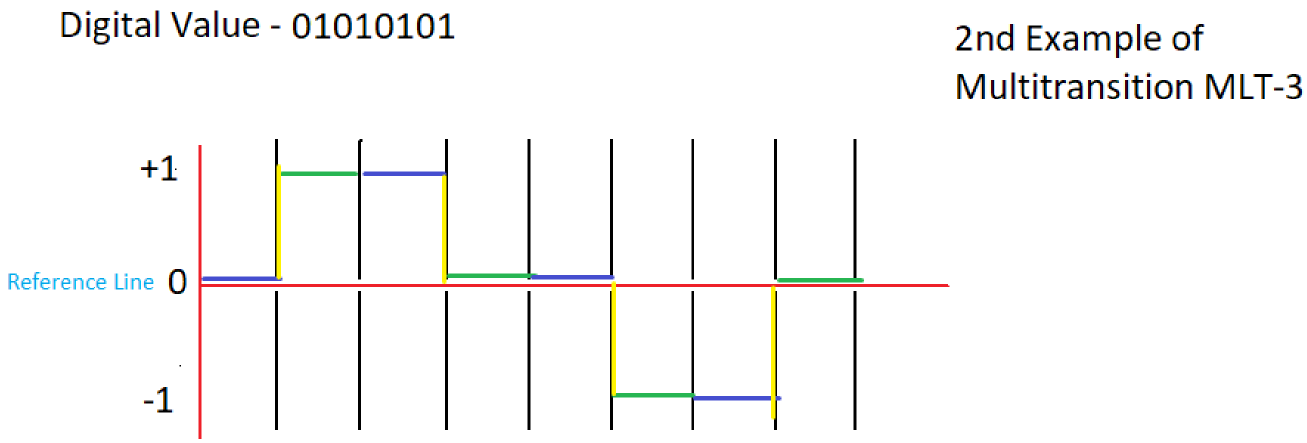


Multitransition - MLT-3
(Multi Level Transmit-3)

1. It uses 3 voltage level
+ve, Nutral, -ve(+1,0,-1)
2. Used in telecom.
3. Generates less Ele. field

Key points for coding:

1. Very first 0 - Nutral
2. Next 0 will depend on 1 and continue 1 signal level.
3. First 1 will always +ve, second 1 nutral, 3rd 1 will be -ve, 4th 1 nutral, 5th 1 +ve, 6th 1 nutral and so on.

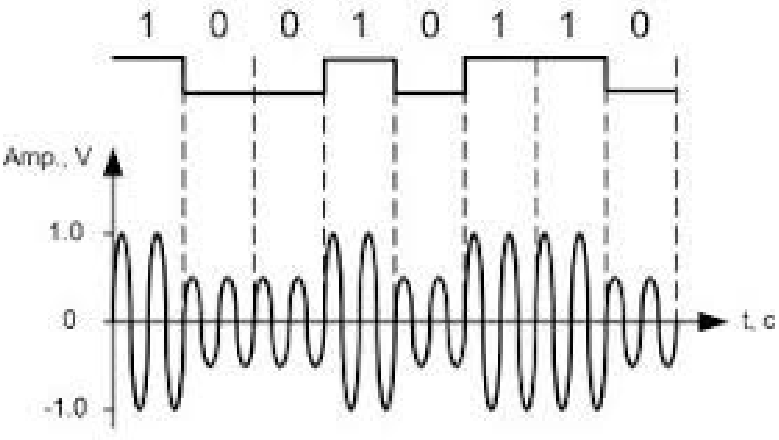


i. 1.

Digital-to-analog conversion

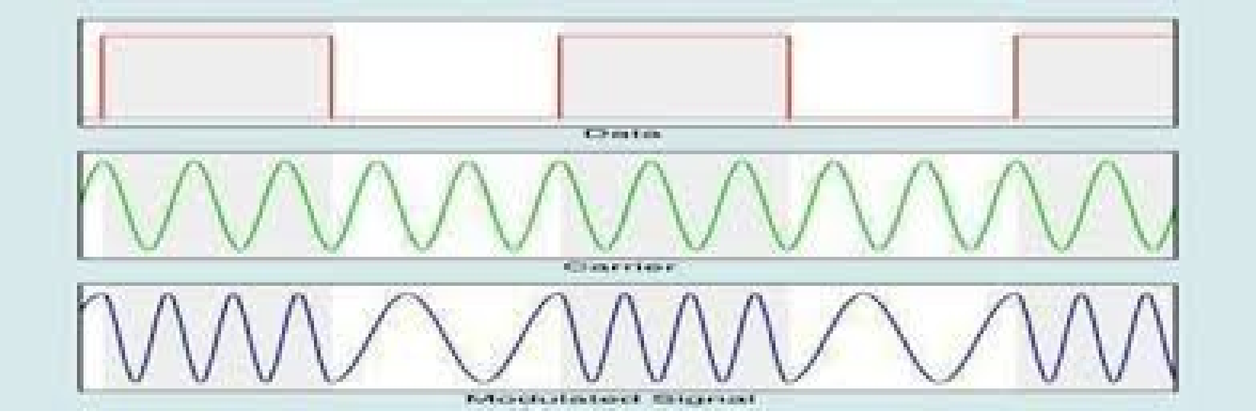
Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal like frequency, Amplitude and phase based on the information in digital data.

1. ASK (Amplitude Shift Keying)
   In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes.

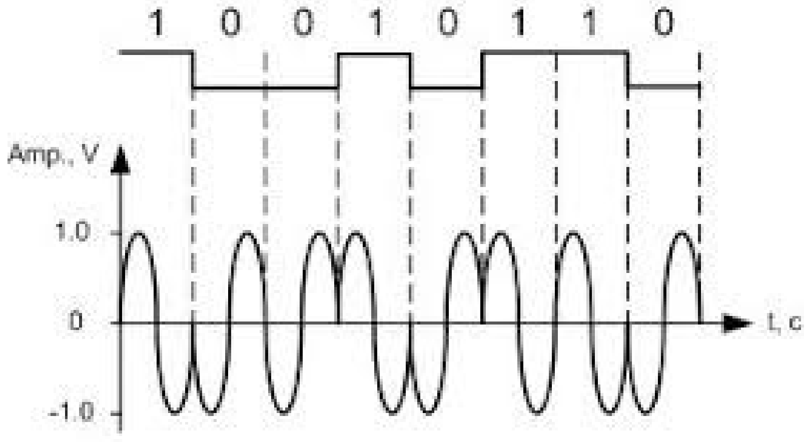


Amplitude shift keying (ASK)

2. FSK(Frequency Shift Keying)
In frequency shift keying, the frequency ofthe carrier signal is varied to represent data. The frequency of the modulated signal is constant for the duration of one signal ele- ment, but changes for the next signal element if the data element changes. Both peak amplitude and phase remain constant for all signal elements.

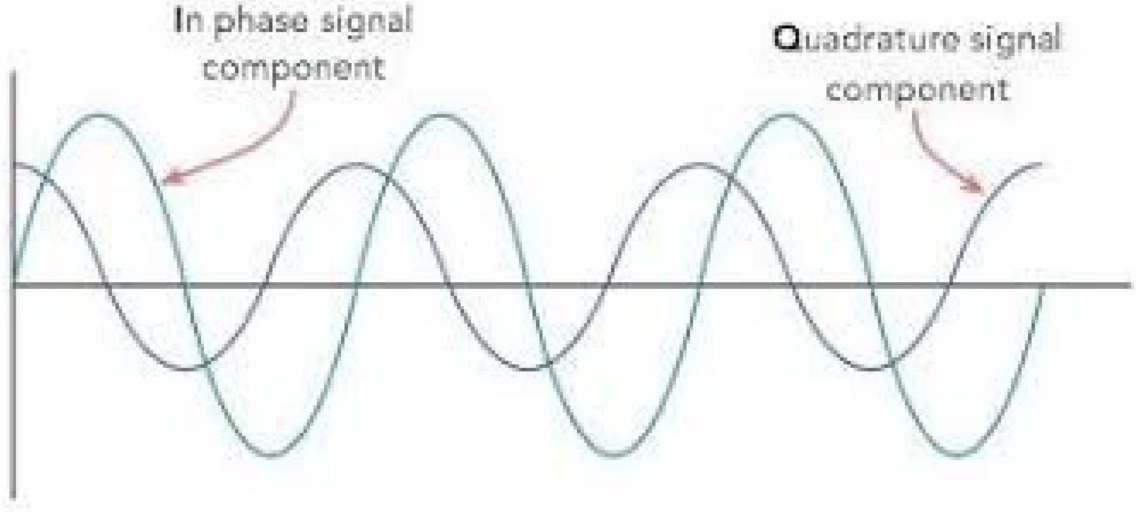


3. PSK (Phase Shift Keying)
In phase shift keying, the phase ofthe carrier is varied to represent two or more differ- ent signal elements. Both peak amplitude and frequency remain constant as the phase changes.



Phase shift keying (PSK)

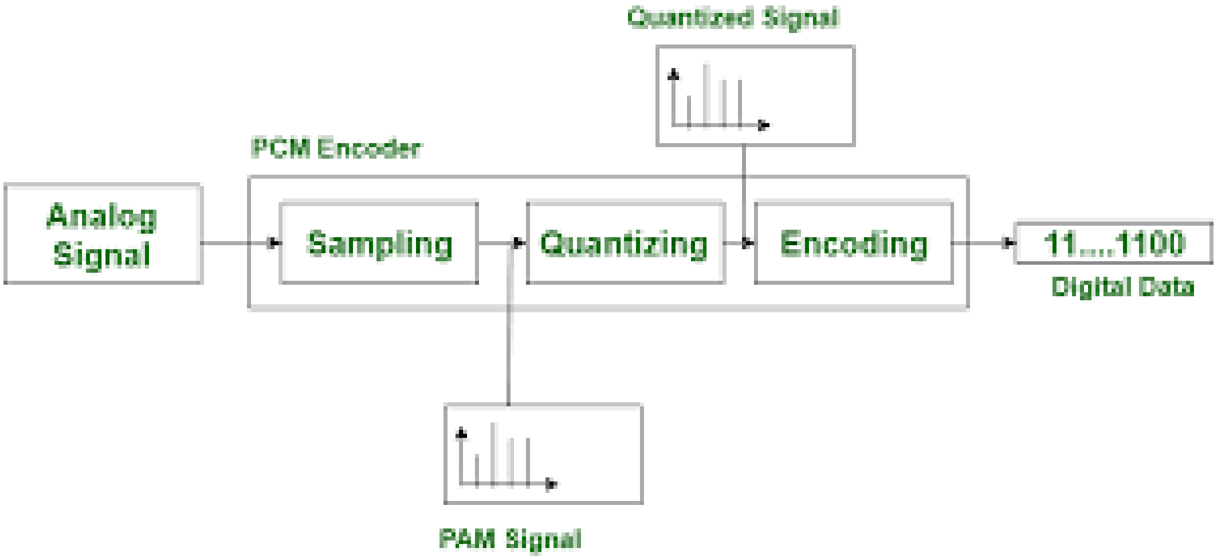
4. QAM(Quadrature Amplitude Modulation)
   PSK is limited by the ability of the equipment to distinguish small differences in phase. This factor limits its potential bit rate. So far, we have been altering only one of the three characteristics of a sine wave at a time; but what if we alter two? Combination of ASK and PSK. The idea of using two carriers, one in-phase and the other quadrature, with different amplitude levels for each carrier is the concept behind quadrature amplitude modulation (QAM).



ANALOG-TO-DIGITAL CONVERSION

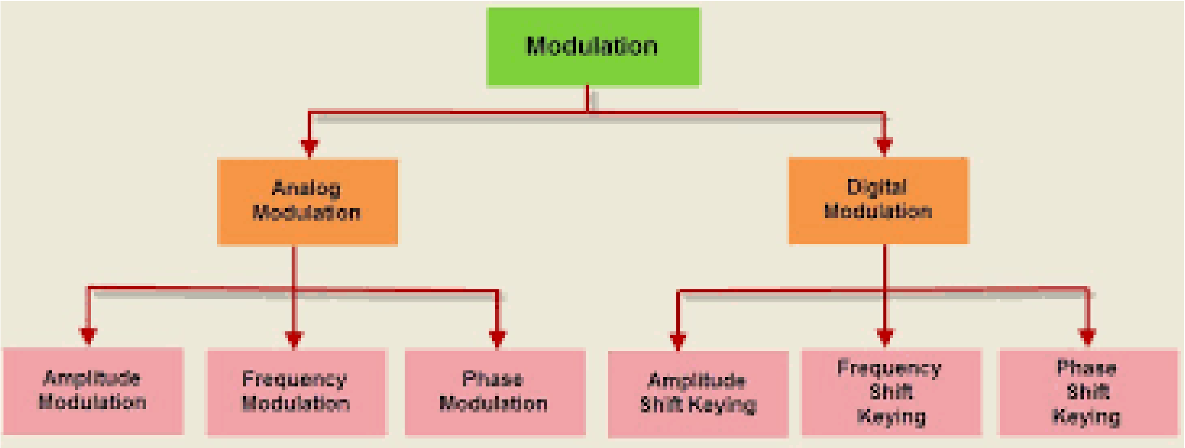
A process to change analog signal to digital signal is known as Pulse Code Modulation (PCM)

Analog Signal ---→ Sampling --→ Quantization --→ Encoding --→ Digital Signal

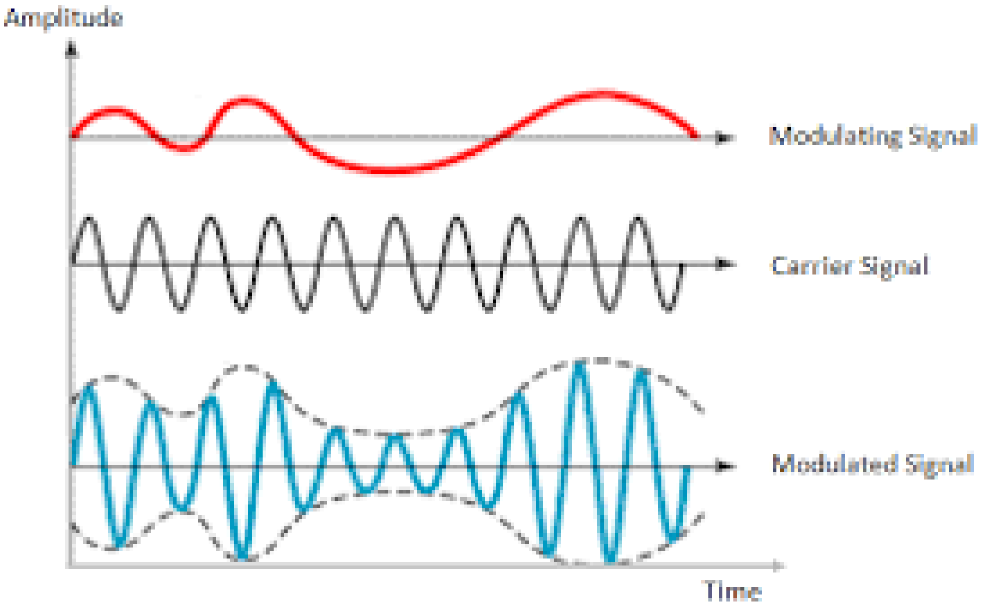


Block Diagram Of PCM

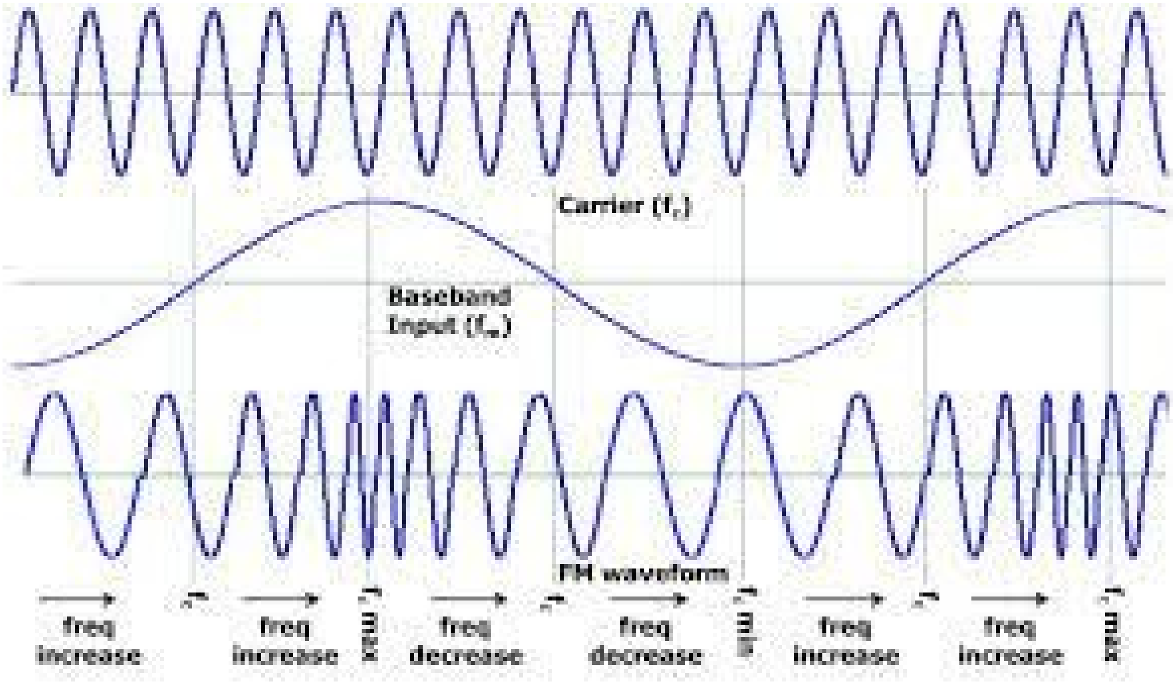
ANALOG-TO-ANALOG CONVERSION



Amplitude Modulation



Frequency Modulation



Pulse Modulation

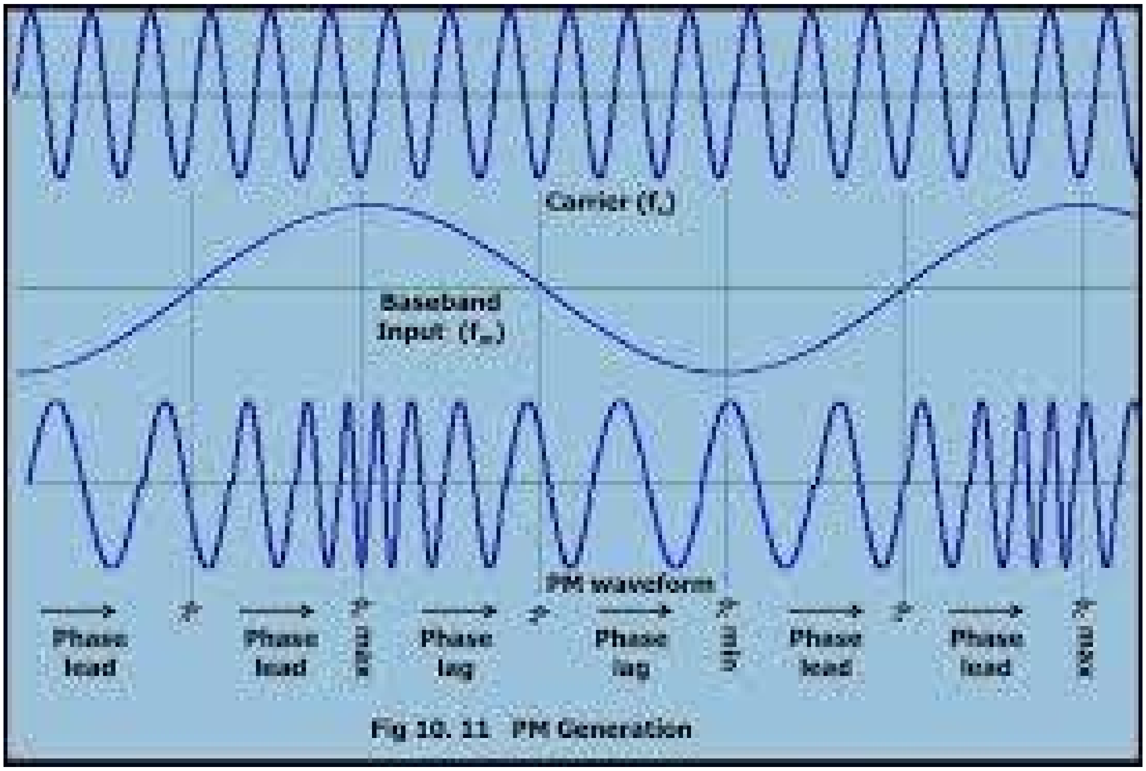


Fig 10. 11 PM Generation

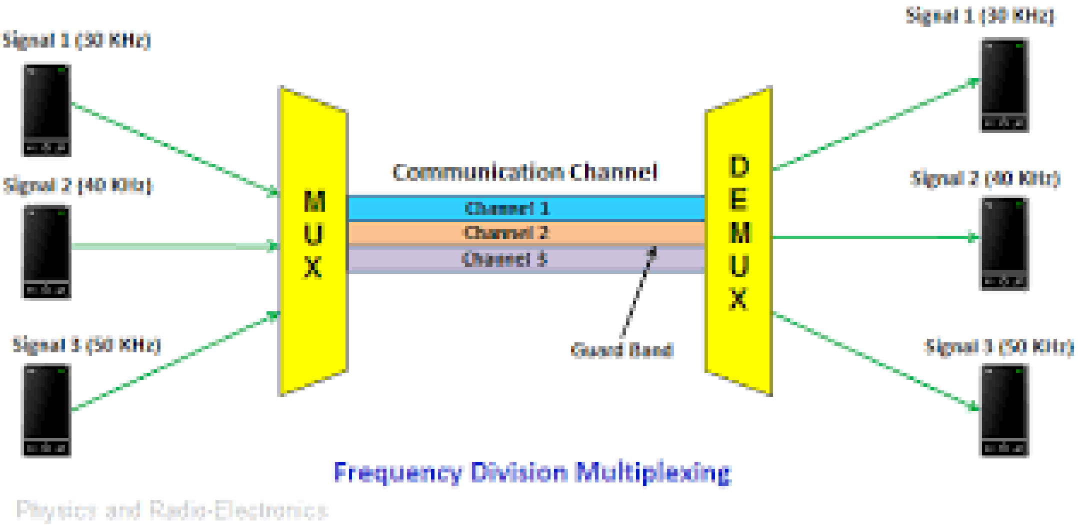
Multiplexing & De-multiplexing

Multiplexing means combining multiple signal into single signal and **De-multiplexing** means breaking multiplexed signal into multiple signal.

Types and description:->

Frequency-Division Multiplexing

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies. Example: Radio, Television, GSM



Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.WDM is conceptually the same as FDM, except that the multiplexing and de-multiplexing involve optical signals transmitted through fiber optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Example: Fiber Optic Cable

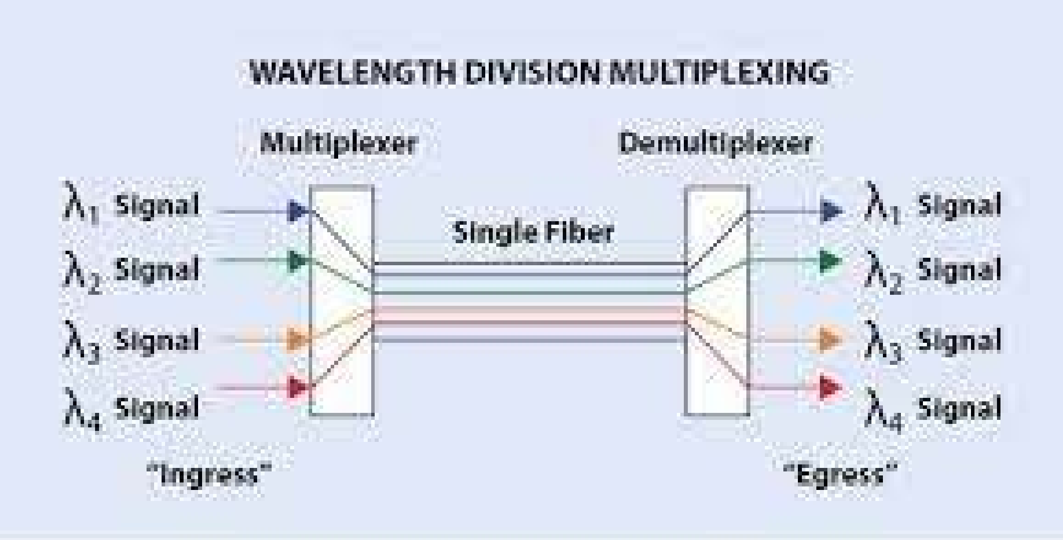
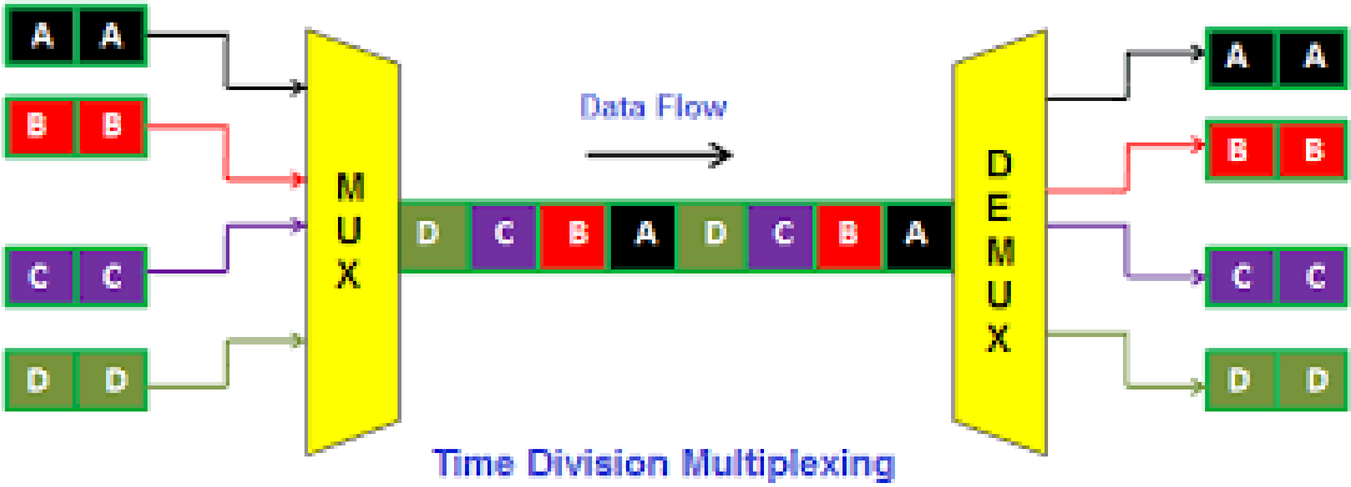


Figure 1: Basic WDM Technology Diagram

Time-devision Multiplexing

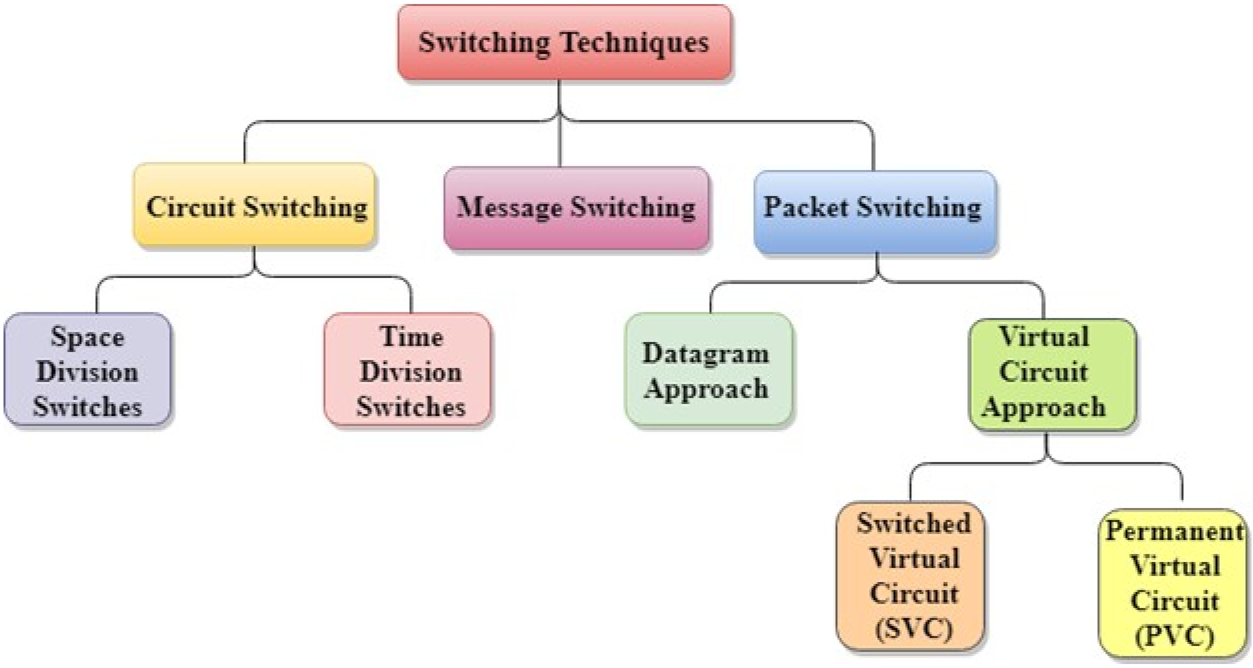
Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a line Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Figure 6.12 gives a conceptual view of TDM. Note that the same link is used as in FDM; here, how- ever, the link is shown sectioned by time rather than by frequency. In the figure, portions of signals 1,2,3, and 4 occupy the link sequentially.

Example: GSM (Global System for Mobile Communication)



Switching

Switching is the technique by which nodes control or switch data to transmit it between specific points on a network.



Circuit Switching :

In circuit switching network resources (bandwidth) are divided into channels for dedicated connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.

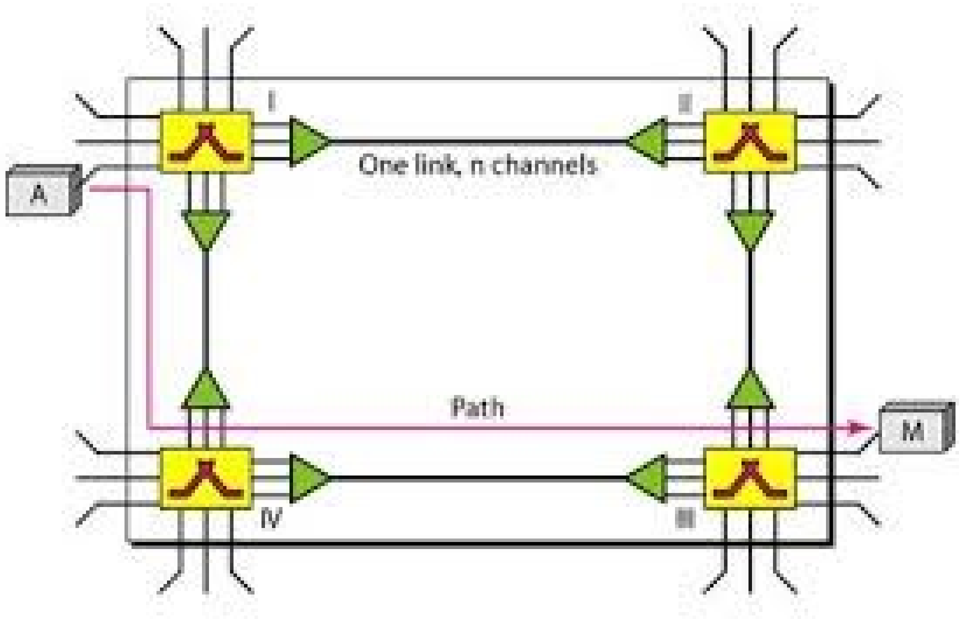
Switched based network and Telephone system network are examples of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.

Advantages of Circuit Switching:

1. The main advantage of circuit switching is that a committed transmission channel is established between the computers which give a guaranteed data rate.
2. In-circuit switching, there is no delay in data flow because of the dedicated transmission path.

Disadvantages of Circuit Switching:

1. It takes a long time to establish a connection.
2. More bandwidth is required in setting up dedicated channels.
3. It cannot be used to transmit any other data even if the channel is free as the connection is dedicated to circuit switching.



Packet switching

Packet switching is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed. Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first stores that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of sources and destinations. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different paths possible over an existing network.

Advantage of Packet Switching over Circuit Switching :

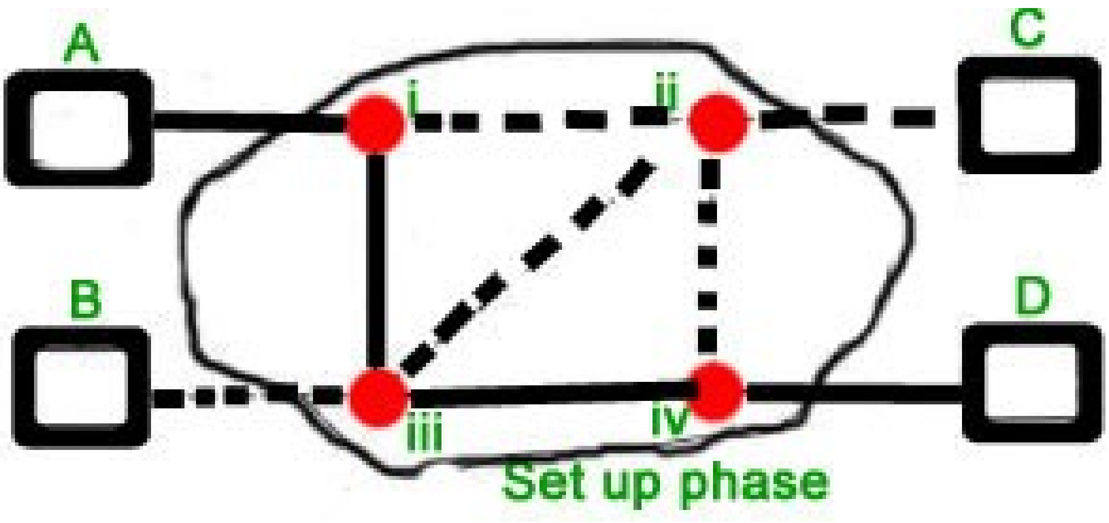
- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as a destination can detect the missing packet.
- More fault tolerant because packets may follow a different path in case any link is down, Unlike Circuit Switching.
- Cost-effective and comparatively cheaper to implement.

The disadvantage of Packet Switching over Circuit Switching :

- Packet Switching doesn't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers for each packet.
- Complexity is more at each node because of the facility to follow multiple paths.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

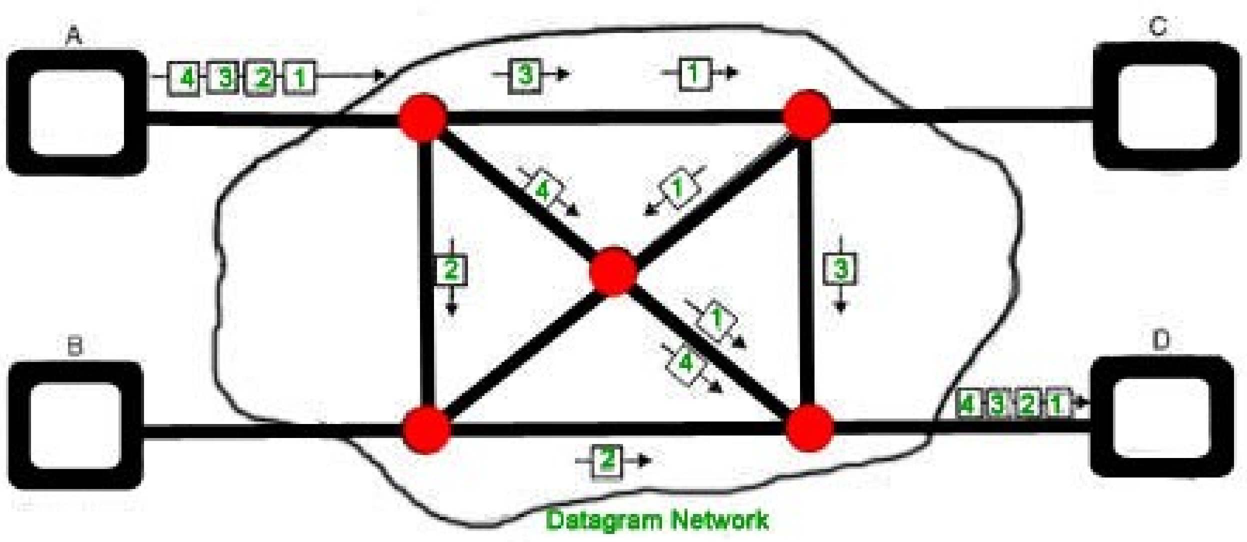
Modes of Packet Switching :

1. **Connection-oriented Packet Switching (Virtual Circuit) :**
   Before starting the transmission, it establishes a logical path or virtual connection using signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence numbers. Overall, three phases take place here- The setup, data transfer and tear down phase.



All address information is only transferred during the setup phase. Once the route to a destination is discovered, entry is added to the switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number, etc. Connection-oriented switching is very useful in switched WAN. Some popular protocols which use the Virtual Circuit Switching approach are X.25, Frame-Relay, ATM, and MPLS(Multi-Protocol Label Switching).

2. **Connectionless Packet Switching (Datagram) :** Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers, etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at the destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.
   Packet delivery is not guaranteed in connectionless packet switching, so reliable delivery must be provided by end systems using additional protocols.



Datagram Packet Switching

Message Switching –

Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced. In message switching, end-users communicate by sending and receiving *messages* that included the entire data to be shared. Messages are the smallest individual unit.

Also, the sender and receiver are not directly connected. There are a number of intermediate nodes that transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems.

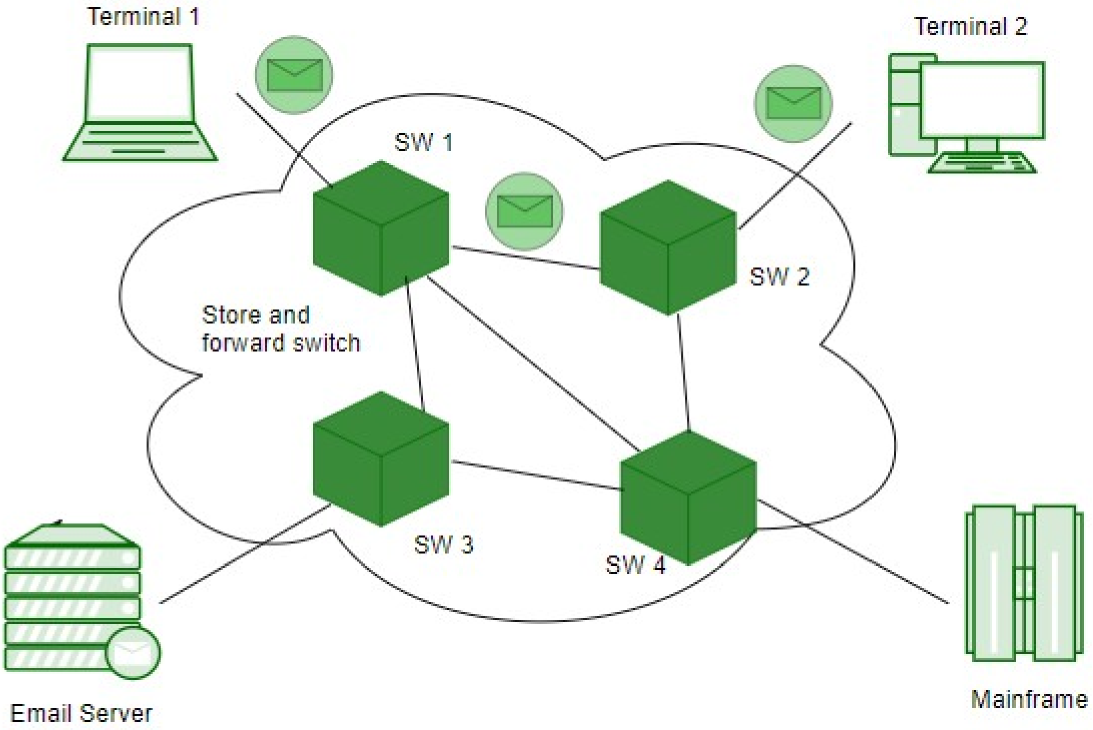
They provide 2 distinct and important characteristics:

1. **Store and forward –** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise, it’ll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is

accepting data. This is called the store-and-forward property.

2. **Message delivery –** This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.

Message switching network consists of transmission links (channels), store-and-forward switch nodes, and end stations as shown in the following picture:



Characteristics of message switching –

Message switching is advantageous as it enables efficient usage of network resources. Also, because of the store-and-forward capability of intermediary nodes, traffic can be efficiently regulated and controlled. Message delivery as one unit, rather than in pieces, is another benefit.

However, message switching has certain disadvantages as well. Since messages are stored indefinitely at each intermediate node, switches require a large storage capacity. Also, these are pretty slow. This is because at each node, first there is a wait till the entire message is received, then it must be stored and transmitted after processing the next node and links to it depending on availability and channel traffic. Hence, message switching cannot be used for real-time or interactive applications like a video conference.

Advantages of Message Switching –

Message switching has the following advantages:

1. As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in the network.
2. In message switching, the data channels are shared by the network devices.
3. It makes traffic management efficient by assigning priorities to the messages.

Disadvantages of Message Switching –

Message switching has the following disadvantages:

1. Message switching cannot be used for real-time applications as storing messages causes delay.
2. In message switching, the message has to be stored for which every intermediate device in the network requires a large storing capacity.

Applications –

The store-and-forward method was implemented in telegraph message switching centers. Today, although many major networks and systems are packet-switched or circuit-switched networks, their delivery processes can be based on message switching. For example, in most electronic mail systems the delivery process is based on message switching, while the network is in fact either circuit-switched or packet-switched.

Telephone Network:

Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, which is referred to as the plain old telephone system (POTS), was originally an analog system using analog signals to transmit voice. With the advent of the computer era, the network, in the 1980s, began to carry data in addition to voice. During the last decade, the telephone network has undergone many technical changes. The network is now digital as well as analog.

Dialup Modem

The term modem is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A modulator creates analog signal from binary data. A demodulator recovers the binary data from the modulated signal.

Digital Subscriber Line (DSL)

After traditional modems reached their peak data rate, telephone companies developed another technology, DSL, to provide higher-speed access to the Internet. Digital subscriber line (DSL) technology is one of the most promising for supporting high-speed digital communication over the existing local loops. DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL). The set is often referred to as xDSL, where x can be replaced by A, V, H, or S.

Technology	downstream	Upstream	Distance(ft)	Twisted Pair	Line Coding
ADSL	**1.5-6.1 Mbps**	**16-640 kbps**	**12000**	**1**	**DMT**
HDSL	**1.5-2.0 Mbps**	**1.5-2.0 Mbps**	**12000**	**2**	**2B1Q**
SDSL	**768 kbps**	**768 kbps**	**12000**	**1**	**2B1Q**
VDSL	**25-55 Mbps**	**3.2 Mbps**	**3000-10000**	**1**	**DMT**